



Technology that **empowers.**

## Hackers, Ransomware, and Data Leaks— Can Your Nonprofit Afford the Risk?

Understanding cyber threats and risk management strategies  
Greg Bugbee, CISSP, CISO

**novus**insight.com



# Agenda Items


- Introductions
- The Big Scaries!
- Understanding Cyber Threats Facing Nonprofits
- Financial Impact of a Cyber Incident
- Assessing and Reducing Cyber Risk
- Cyber Insurance and Risk Management
- Actionable Strategies for Cyber Protection
- Wrap up and Q&A



# Tell us what you think:

- What is the number one catastrophic cyber incident that could happen?
- What is it about the scenario that makes it catastrophic?
- What are you currently doing to protect yourself from this catastrophic thing from happening?



The background is a deep blue gradient. A series of glowing, wavy lines composed of small white and light blue dots flow horizontally across the upper half of the image. Scattered throughout the entire background are numerous small, out-of-focus white and light blue specks, resembling dust or distant stars.

# Overview of the Blue Hills Civic Association Cyber Fraud Incident



# Incident Description

## Wire Transfer Fraud Scheme

In December of 2024, the Blue Hills Civic Association fell victim to a complex wire transfer fraud, highlighting vulnerabilities in financial and incident response processes.

## Organizational Crisis

The incident led to an organizational crisis, threatening the stability and future of the BHCA.

## Impact on the Nonprofit and the Community

The fraud not only caused financial loss but also affected the trust and operation of the nonprofit. In addition, programs such as a summer youth employment program, were forced to be cancelled, resulting in massive ripple effects throughout the community.



# Details of the Fraud

---



# Fraud Occurrence

## **Federal Pandemic Relief Grant**

BHCA managed a \$5 million grant funded by federal pandemic relief programs to support community development.

## **Cybercriminal Impersonation Scheme**

BHCA fell victim to a cybercriminal impersonation scheme that led to the diversion of approximately \$300,000 in funds.

## **Importance of Security in Fund Management**

Effective security measures are crucial in managing grants and funds transfer to prevent fraud and ensure that funds reach intended recipients.



---

# Delayed Notification and Consequences

## **Timing of Notification**

The delayed notification of fraud significantly impacted internal and external stakeholders, causing confusion and distrust.

## **Contractual Violations**

Failure to notify within the required timeframe constituted a violation of contractual obligations, leading to the State of Connecticut withholding funding from the nonprofit.

## **Funding Consequences**

The trust erosion due to delayed communication resulted in immediate consequences for funding and financial operations.



---

# **Impact on BHCA**

---

# Funding and Staff Layoffs

## Funding Suspension

DECD (Department of Economic and Community Development) has suspended all current and future payments to BHCA, significantly impacting its operations.

## Employee Layoffs

Due to the lack of operating funds, nearly all 30 employees at BHCA were terminated, affecting team dynamics and the organization's ability to serve to community.



# Operational and Reputational Damage



## Operations Halted

Programs were paused, resulting in significant disruption of community services and operational activities.



## Reputation Damaged

Intensified media scrutiny and legislative pressures led to the erosion of trust among donors and the public.



## Investigations Launched

Formal investigations by both the FBI and Hartford Police initiated, increasing the urgency and seriousness of the situation.



---

# Critical Failures

---

---

# Lack of Wire Transfer Controls

## **Inadequate Verification Procedures**

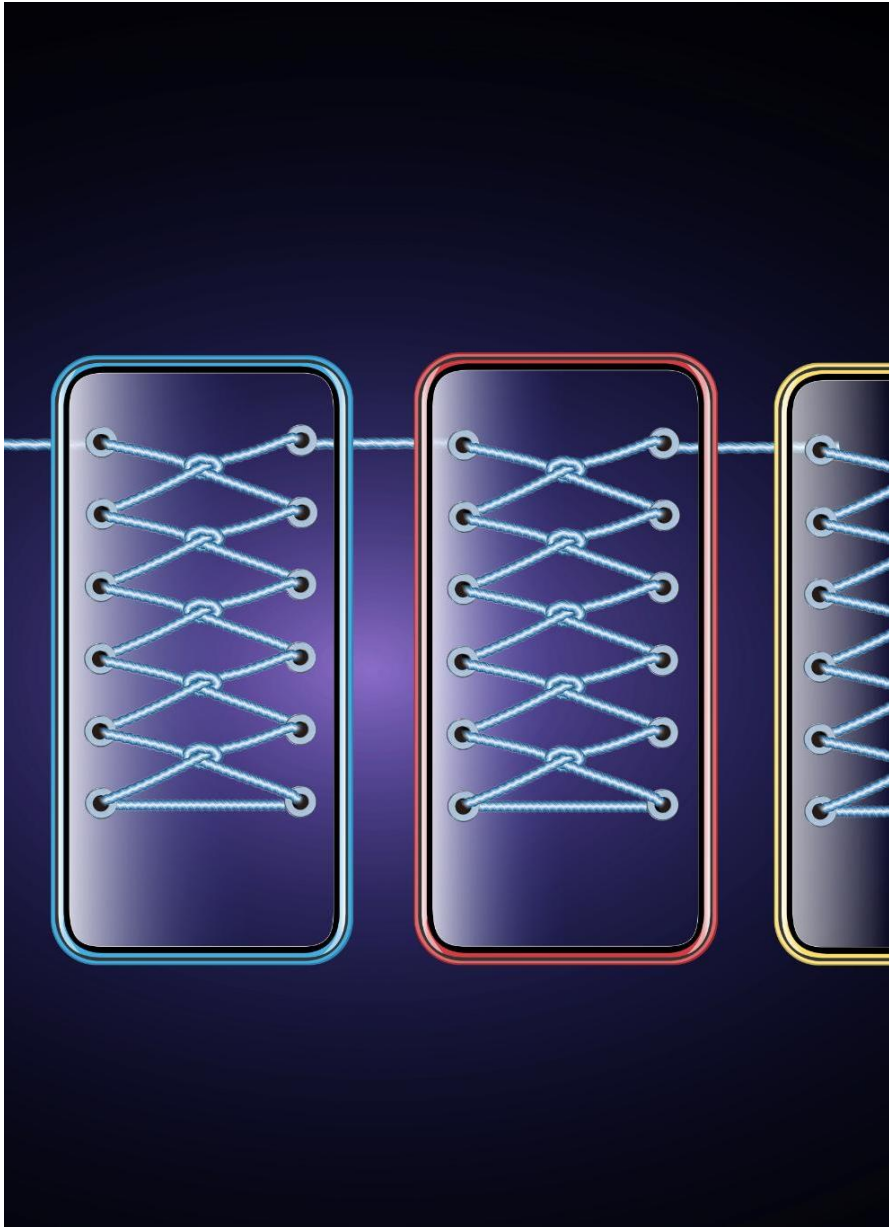
BHCA lacked sufficient internal procedures for verifying large wire transfers, which increases the risk of fraud.

## **Importance of Dual Authorization**

Implementing dual authorization could enhance security and prevent unauthorized wire transfers.

## **Callback Procedures**

Utilizing callback procedures can help verify the authenticity of large wire transfer requests, reducing the risk of fraud.



---

# Unawareness of Contractual Obligations

## Importance of Disclosure

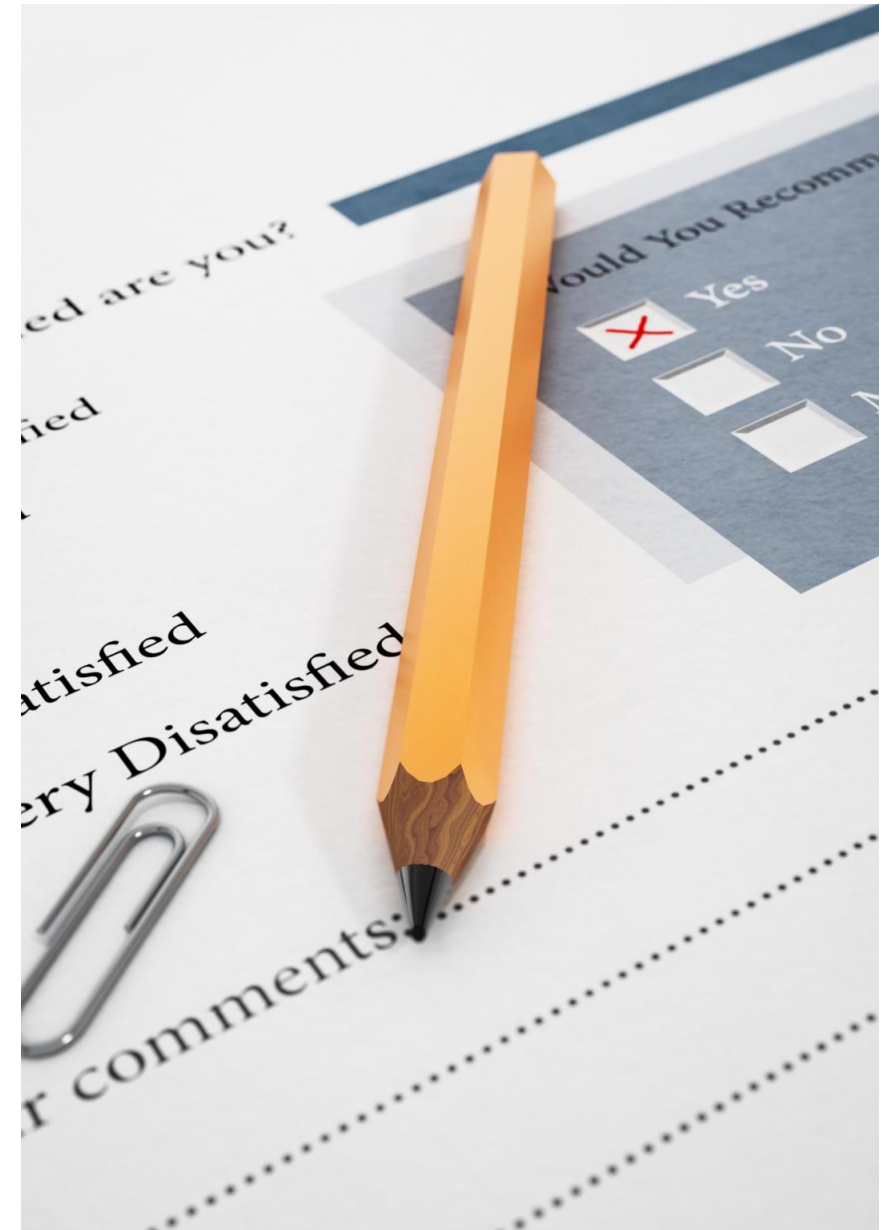
Grant contracts necessitate timely disclosure of any potential misuse or loss of funds to ensure accountability.

## Consequences of Delay

Delays in reporting can lead to severe ramifications, including suspension of funds and demands for clawbacks.

## Understanding Contractual Clauses

A clear understanding of contractual obligations is essential to prevent violations and protect fund integrity.





# No Formal Incident Response Plan

## Impact of Delays

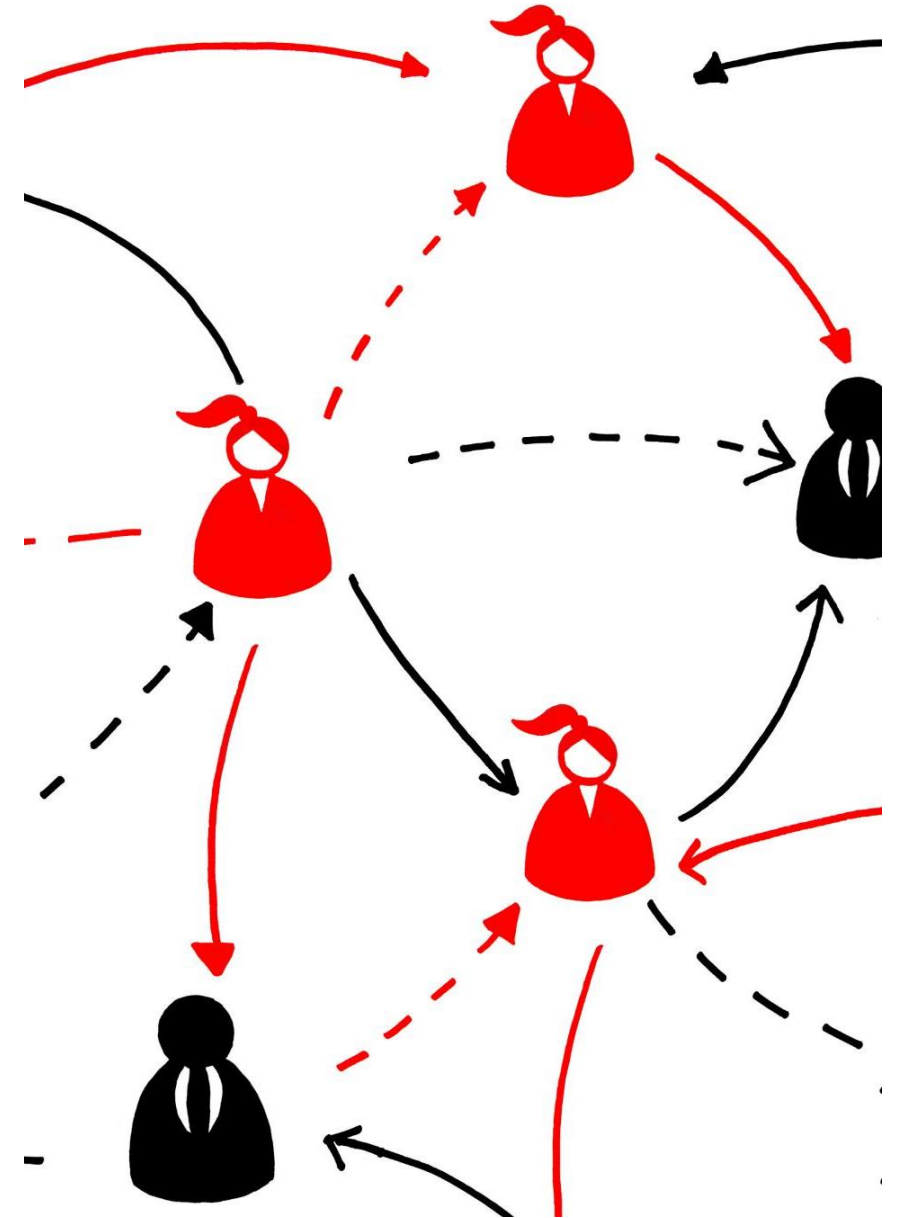
Delays in response significantly worsened the overall impact of the incident, highlighting the need for efficient communication.

## Importance of Planning

Having a documented incident response plan would ensure timely notifications and proper containment measures to mitigate damage.

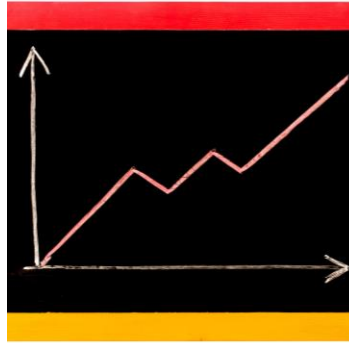
## Guidance for the Team

A practiced response plan would provide clear guidance to the team, improving coordination during critical situations.



---

# Lack of Cyber Insurance



## Financial Impact of Cyber Attacks

Without cyber insurance, entities face significant financial losses due to cyber attacks, including recovery and legal costs.



## Importance of Cyber Insurance

Cyber insurance can mitigate costs associated with investigations and legal exposure, providing essential financial support during crises.



## Risk Management Strategies

The absence of a cyber insurance policy represents a gap in risk management strategies, leaving organizations vulnerable.

# Lessons for Nonprofit Leaders

---



---

# Importance of Cybersecurity

## Cybersecurity Awareness

Nonprofits must understand that they are viable targets for cybercriminals. Awareness is the first step to protection.

## Vulnerability of Nonprofits

Many nonprofits lack robust cybersecurity measures, making them attractive targets for cyber-attacks. In this case, two nonprofits fell victim to a cyber-attack- Blue Hills and the nonprofit that experienced the initial email compromise.

## Need for Strong Defenses

Implementing strong cybersecurity defenses is essential for nonprofits to protect sensitive data and maintain trust.





---

# Policy and Training Investment

## **Written Financial Policies**

Establishing clear written policies for financial transactions is essential to prevent unauthorized transfers and fraud.

## **Regular Staff Training**

Regular training sessions equip staff with the skills needed to recognize and respond to fraud attempts effectively.

## **Fraud Recognition Techniques**

Training staff on specific fraud recognition techniques helps in identifying potential threats like business email compromise.

## **Acceptable Use Program**

Establish guidelines for responsible and ethical use of IT resources to protect sensitive information and ensure compliance with policies.

# Incident Response Plan

## Define Response Protocols

Establish clear protocols for responding to cyber events to ensure a coordinated and effective response.

## Timely Communication

Identify key contacts and define timelines for communication with the board, funders, and law enforcement during an incident.

## Practice the Plan

Regularly practice the incident response plan to ensure all team members are prepared and aware of their roles.







---

# Understanding Contracts

## **Importance of Reading Contracts**

Understanding your contracts is crucial to ensure compliance and protect your funding opportunities.

## **Breach Notification Requirements**

Many agreements include specific breach notification requirements that must be adhered to avoid jeopardizing funding.



---

# Cyber Insurance

## **Comprehensive Coverage**

A cyber insurance policy can provide comprehensive coverage, including loss coverage, for various incidents, ensuring your organization is protected from unexpected events.

## **Forensic Costs and Legal Fees**

Cyber insurance can help cover forensic investigation costs and legal fees associated with data breaches and cyber incidents.

## **Regulatory Fines and PR Support**

In the event of a breach, cyber insurance can assist with regulatory fines and provide public relations support to manage reputation.



---

# Immediate Steps for Nonprofits

## **Develop an Incident Response Plan**

Creating a formal incident response plan is crucial for nonprofits to effectively handle cyber threats and incidents.

## **Establish Wire Transfer Procedures**

Implementing secure wire transfer procedures can help prevent financial fraud and enhance organizational security.

## **Obtain Cyber Insurance**

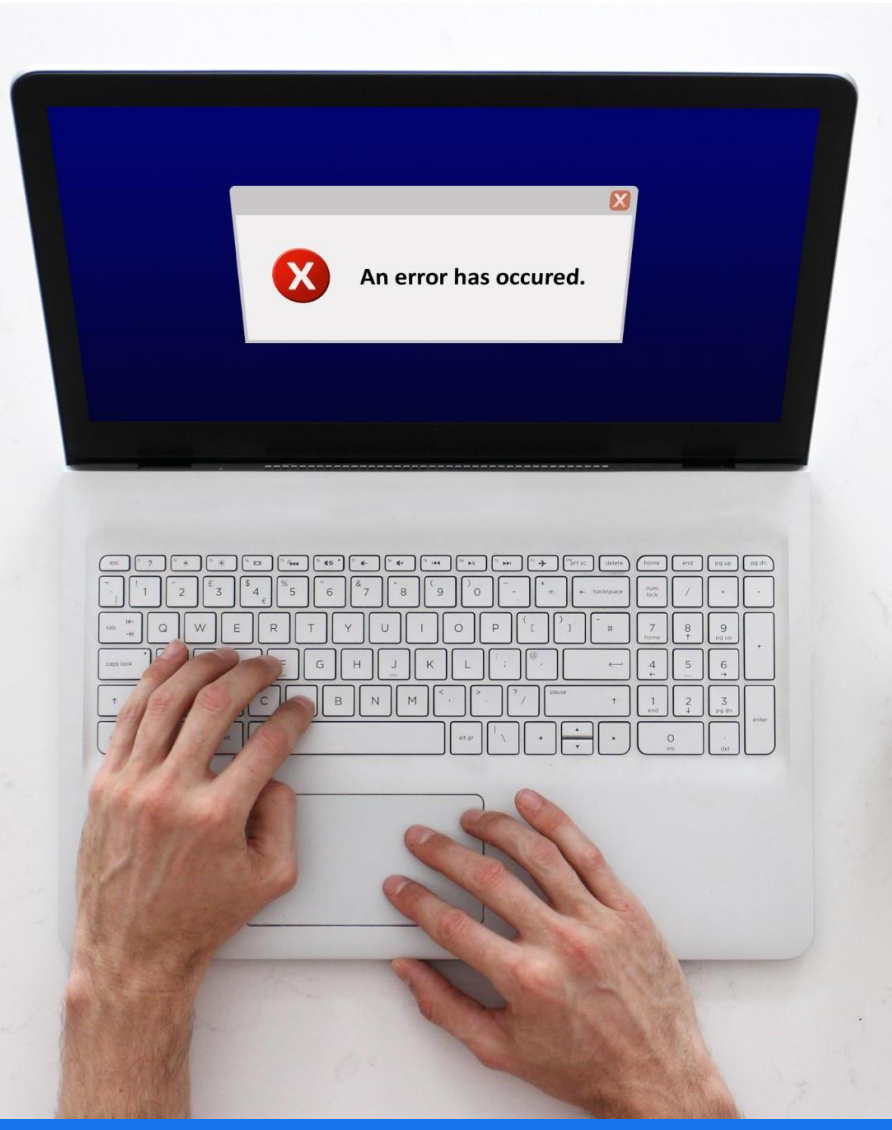
Acquiring a cyber insurance policy provides financial protection against the costs associated with data breaches and cyber incidents.



# Understanding Cyber Threats Facing Nonprofits

---





# Types of Cyberattacks Targeting Nonprofits

## Phishing Attacks

Phishing attacks often target nonprofits through deceptive emails, aiming to steal sensitive information

## Ransomware Attacks

Ransomware attacks can lock nonprofit organizations out of their data, demanding payment for restoration of access.

## Data Breaches

Data breaches expose sensitive information, leading to data loss and potential legal issues for nonprofits.





# Why are nonprofits attacked?

Everyone is a target, and an org isn't too small or not valuable enough to attack- if there's a dollar to steal, someone wants to steal it.

Budget challenges- yeah, there's that pesky overhead thing again. The reality is that you have to protect data or meet certain obligations to run a program, then those costs are direct program expenses.

Valuable data- Medical information, employee data, donor data, and more...

Hacktivism- Nonprofits may be targets due to the causes they represent

Trusted access to others- Nonprofits can provide access to larger targets through their connections- wealthy donors, government organizations, other nonprofits, and funders.

# Reputational Damage and Loss of Donor Trust

## Impact of Cyber Incidents

Cyber incidents can severely damage an organization's reputation, leading to a decline in donor confidence and support.

## Loss of Donor Trust

When trust is compromised, donors may withdraw their support, making fundraising efforts increasingly difficult.

## Long-term Effects

The repercussions of reputational damage can last for years, affecting organizational credibility and future fundraising initiatives.





# Financial Impact of a Cyber Incident

The background of the slide is a dark blue, abstract image featuring various financial data visualizations. It includes multiple overlapping line graphs in shades of blue and red, some with markers. There are also candlestick charts and bar charts visible, though they are blurred and semi-transparent. The overall aesthetic is high-tech and data-driven, with a focus on financial markets.

# The 'Record' of Doom!



- A record is like a digital fingerprint, except less cool.
- It's what hackers dream of – personal data on a platter!
- In cyber terms, a record is anything that can be stolen and shared
- Records have value to attackers and can be bought and sold





# Identifying Your Organization's Records

- What types of records does your organization maintain?
  - Employees
  - Donors
  - People you serve
- How many records do you have?
- Where are they?
- Who has access to them?



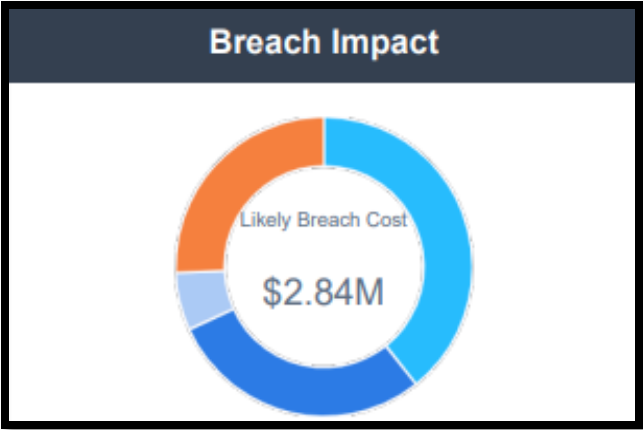
# Risk Scenario: Ransomware Attack

Scenario:

Malicious software encrypts a nonprofits' systems, halting operations and demanding payment for recovery.

Primary Impacts:

- Operational Disruption (immediate halt to services)
- Financial (ransom payment, recovery costs, fines)
- Loss of Productivity (days to weeks of downtime)
- Reputational (visible service outages)
- Legal/Compliance (if data is also exfiltrated)



Industry	Breach Type
Public	Ransomware
Est. Industry Breach Cost	Est. Data Lost
\$2,842,430.09	16,927 records



# Cost Breakdown: Response and Recovery

## Forensic Investigations

Forensic investigations are crucial for understanding the impact of a cyber incident, often leading to significant expenses.

## Legal Fees

Legal fees can quickly accumulate due to the need for compliance with regulations and potential litigation following a cyber incident.

## System Restorations

Restoring affected systems is a critical step in response and recovery, often incurring substantial costs for repairs and updates.

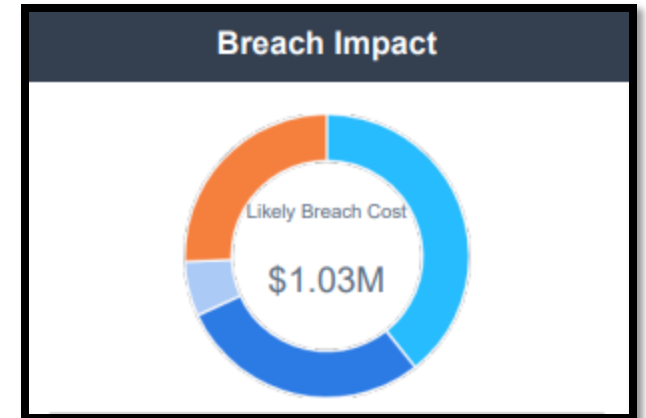
# Risk Scenario: Breach of Personally Identifiable Information (PII)

## Scenario:

*Unauthorized access to client or employee data leads to a data breach of sensitive personal information.*

## Primary Impacts:

- **Legal/Compliance** (breach notifications, regulatory response)
- **Financial** (credit monitoring, breach notification, **regulatory fines**)
- **Reputational** (loss of public trust, media coverage)
- **Identity Theft Risk** (impact to clients or staff)
- **Long-Term Fallout** (oversight investigations, strained donor and client confidence)



Industry	Breach Type
Public	PII Breach
Est. Industry Breach Cost	Est. Data Lost
\$1,030,643.52	1,991 records



# Cyber Insurance and Risk Management





# Understanding Cyber Insurance Coverage



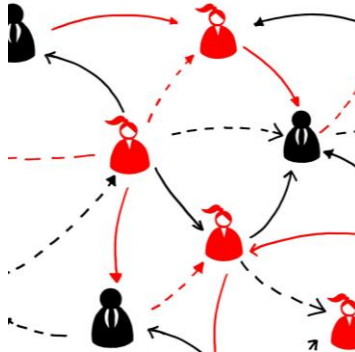
## Coverage for Data Breaches

Cyber insurance provides coverage for expenses resulting from data breaches, including costs for legal representation and notifications.



## Legal Fees and Costs

One of the key benefits of cyber insurance is compensation for legal fees incurred during data breach incidents.



## Public Relations Efforts

Cyber insurance can assist with public relations efforts to mitigate damage and protect an organization's reputation after a breach.



# How Cyber Insurance Can Mitigate Financial Impact



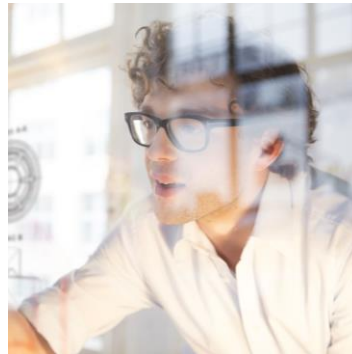
## Reducing Financial Burden

Cyber insurance helps organizations mitigate the financial impact of cyber incidents, providing essential support during crises.



## Resource for Recovery

Cyber insurance offers vital resources and support for businesses to recover quickly from cyber incidents and breaches.



## Maintaining Operational Continuity

Having cyber insurance helps organizations maintain operational continuity, minimizing downtime and disruptions caused by cyber threats.

What does a  
“good”  
policy look  
like?

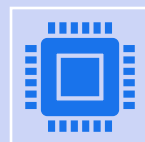
Coverage	START LIMIT	EXAMPLE
Aggregate Limit	\$1,000,000	\$1,000,000
Deductible	\$0	Example
Premium	????	Example
Third Party Coverages		
Privacy and Security Liability	\$50,000	\$1,000,000
Regulatory Fines and Penalties	NOT INCLUDED	\$1,000,000
Notification Costs	\$50,000	\$1,000,000
PCI Fines and Assessments	NOT INCLUDED	\$1,000,000
Multimedia Liability	NOT INCLUDED	\$1,000,000
First Party Coverages		
Breach Response Expenses	\$50,000	\$1,000,000
Ransomware & Extortion Loss	\$50,000	\$1,000,000
Data Replacement and Recovery	NOT INCLUDED	\$1,000,000
Public Relations	\$50,000	\$1,000,000
Business Interruption	NOT INCLUDED	\$1,000,000
Reputation Damage	NOT INCLUDED	\$1,000,000
Dependent Network Interruption	NOT INCLUDED	\$1,000,000
Dependent System Failure	NOT INCLUDED	\$1,000,000
Hardware Replacement Costs/Betterment	NOT INCLUDED	\$1,000,000
Crime Coverages		
Electronic Theft (Funds Transfer)	\$20,000	\$100,000-\$250,000
Social Engineering	NOT INCLUDED	\$100,000-\$250,000
Invoice Manipulation	NOT INCLUDED	\$100,000-\$250,000
Telephone Fraud	NOT INCLUDED	\$100,000-\$250,000
Cryptojacking	NOT INCLUDED	\$100,000-\$250,000



Premiums are based on a number of factors, including revenue



Your "Business Obligations" are another. HIPAA covered entity? Expect to pay more.



Security controls reduce risk and premium, allowing your organization to be in front of more insurance carriers. Competition reduces rates.



Most \$1,000,000 aggregate policies are between \$2000 and \$8000 for annual premium.

How much  
should I expect  
to spend?

---

How do I get insured and save money on my insurance?

The path to cyber insurability



## Step 1: Understand Your Risk

Why it matters: Knowing where you're vulnerable helps you fix problems before they happen and shows insurers, you're serious about security.

Key action: Identify your biggest risks and write them down. Focus on your most important systems and data.

## Step 2: Know Your Assets

Why it matters: You can't protect what you don't know you have. Insurers expect you to keep track of your systems, data, and devices.

Key action: Make a list of your computers, software, and sensitive data. Keep it updated.



---

# 8 Cyber insurance essentials



## Multi-Factor Authentication (MFA)

Why it matters: Stops hackers from getting in even if they steal a password.

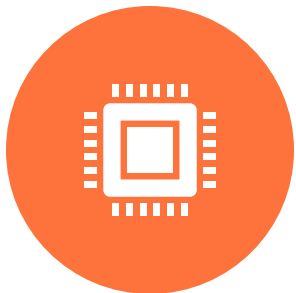
Key action: Turn on MFA for email, sensitive systems, and anything used remotely.



## Backup and Recovery

Why it matters: Ensures you can recover your data if something goes wrong, like ransomware.

Key action: Back up your data regularly and test that you can restore it.



## Endpoint Detection and Response (EDR)

Why it matters: Helps you quickly find and stop cyber threats on your computers.

Key action: Use tools to monitor and respond to suspicious activity on devices.



## Email Filtering

Why it matters: Blocks dangerous emails that could trick employees or spread malware.

Key action: Use email filters to catch phishing and malicious emails before they reach inboxes.

---

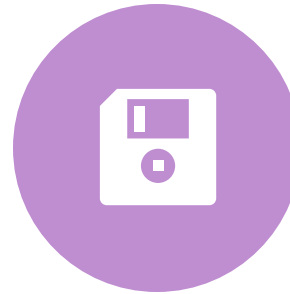
# 8 Cyber insurance essentials



## Patch and Vulnerability Management

Why it matters: Fixes weak spots in your software before hackers exploit them.

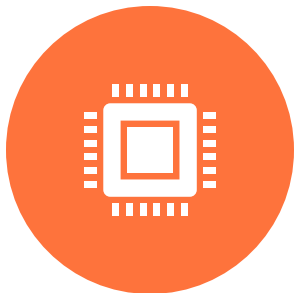
Key action: Regularly update your systems and software.



## Security Awareness Training

Why it matters: Employees who recognize cyber threats make fewer mistakes.

Key action: Train your staff on spotting phishing emails and other scams.



## Incident Response Plan

Why it matters: Having a plan reduces chaos and speeds up recovery during a cyberattack.

Key action: Write down what to do if there's an attack and practice the plan.



## Funds Transfer Policy

Why it matters: Prevents fraud by requiring checks before transferring money.

Key action: Always double-check large payments with multiple people..



# Actionable Strategies for Cyber Protection

# Developing a Comprehensive Cyber Security Program



Establish Governance– Boards and Executives are Accountable for Cyber Programs; IT is responsible for executing



## Security Policies

Establishing clear security policies is essential for guiding employees' actions and protecting organizational assets.



## Response Procedures

Developing effective response procedures ensures quick action during security incidents to minimize damage and restore normal operations.



## Proactive Risk Management

A proactive approach to risk management involves identifying potential threats and vulnerabilities before they escalate into significant issues.





# Practical Tools and Resources for Nonprofits

## Security Software

Nonprofits should invest in security software to safeguard their sensitive information from cyber threats and data breaches. Check out the Microsoft donation program at [Techsoup.org](https://techsoup.org). The **Business Premium plan** for Microsoft 365 has just about everything needed for the foundation of a modern security program. If you're concerned about password management, **Dashlane** is offered on Techsoup. Keeper and Bitwarden are also quality products.

## Training Programs

Implementing training programs for staff can significantly improve awareness and skills related to cybersecurity best practices.

## Resource Accessibility

Utilizing accessible resources helps nonprofits stay informed about the latest cybersecurity threats and defense strategies. What are some of your go to resources for cyber security?

# Conclusion

---

## Evolving Cyber Threats

Cyber threats are constantly changing, making it essential for nonprofits to stay informed and proactive in their cybersecurity measures.

## Prioritizing Cybersecurity

Nonprofits must prioritize cybersecurity to protect sensitive data and resources essential for their operations and mission.

## Effective Communication

Communicating with stakeholders about cybersecurity is vital for building trust and ensuring collaborative efforts in safeguarding resources.



## Q & A

Greg Bugbee, CISSP

Chief Information Security  
Officer

[gbugbee@novusinsight.com](mailto:gbugbee@novusinsight.com)

Novusinsight.com